An Enterprise Continuous Monitoring Technical Reference Model

Jointly developed with the U.S. National Security Agency and the U.S. Department of Homeland Security and NIST

8/30/2011

Presenter: David Waltermire
Security Automation Architect
National Institute of Standards and Technology

Our CM Modeling Design Team

Peter Sell
National Security Agency

Timothy McBride
Department of Homeland Security

Peter Mell, David Waltermire, Harold Booth
National Institute of Standards and Technology

Valery Feldman, Adam Halbardier, Zach Ragland
Booz Allen Hamilton

Alfred Ouyang, Mark Crouter
MITRE

Description of CM applied to Cybersecurity and for use with Technical Reference Models

Continuous security monitoring is a risk management approach to Cybersecurity that maintains an accurate picture of an organization's security risk posture, provides visibility into assets, and leverages use of automated data feeds to measure security, ensure effectiveness of security controls, and enable prioritization of remedies.

Source: NIST IR 7756

Domains that CM can support

1) Vulnerability Management
2) Patch Management
3) Event Management
4) Incident Management
5) Malware Detection
6) Asset Management
7) Configuration Management
8) Network Management
9) License Management
10) Information Management
11) Software Assurance

Additional Proposed Domains:
12) Digital Policy Management
13) Advanced Persistent Threat

Source: NIST SP 800-137

Derived CM Characteristics:

- Maintains an accurate picture of an organization's security risk posture
- Measures security posture
- Identifies deviations from expected results
- Provides visibility into assets
- Leverages automated data feeds
- Ensures continued effectiveness of security controls
- Enables prioritization of remedies
- Informs automated or human-assisted implementation of remedies

Ways to Implement a CM Enterprise Architecture in Your Organization

- Create ad-hoc system
  - Integrating vendor solutions to create a CM capability
  - Duplicating the work and repeating the mistakes of others
- Procure entire CM solutions from a single vendor
  - Locking into a solution that will be strong in some areas and weak in others
- Leverage a **CM technical reference model** and **related security standards** (e.g., SCAP)
  - Leverage your existing security products
  - Reduce integration costs
  - Combine best of breed solutions
  - Enable Federal government-wide interoperable solutions

Technical Challenges to be Addressed by a CM Technical Reference Model

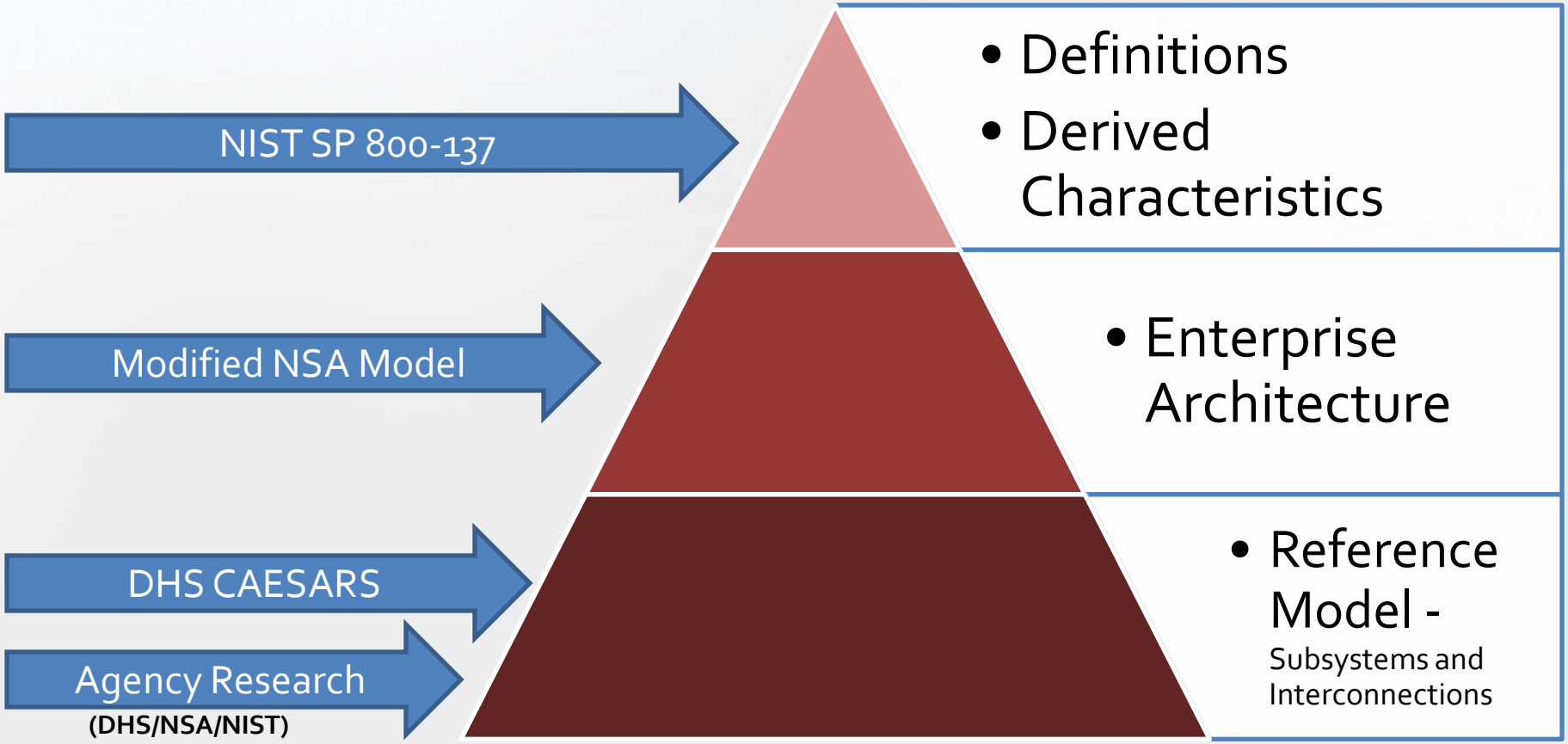
- These are areas that need to be addressed to achieve the enterprise architecture but for which commercial tools are often deficient

- Component based approach
- Creating hierarchical continuous monitoring instances
  - Inter-tier communication
  - Standardized reporting
- Dynamic, ad hoc, or operational queries
- Orchestrated control and tasking of collection systems
- Normalization of collected data
- Need to collect raw data, not results
- Ability to customize analysis and scoring based on current threats and weaknesses

CM Reference Model – NIST IR 7756
Phase 1: Draft completed

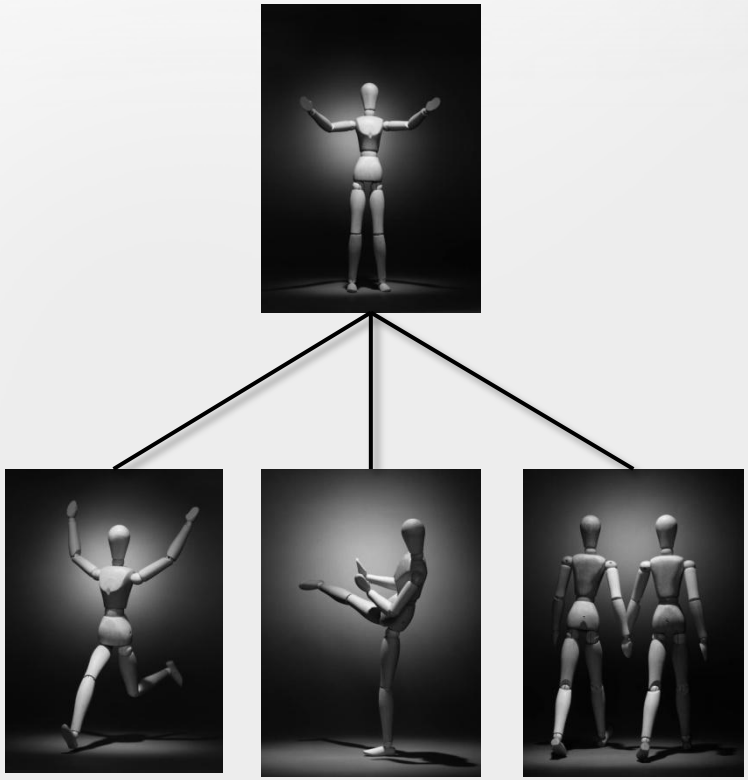
Leveraged Design Sources:

Design Levels:



Architecture Derivations communications

The reference model enables derivation of specific architectures



Reference Model

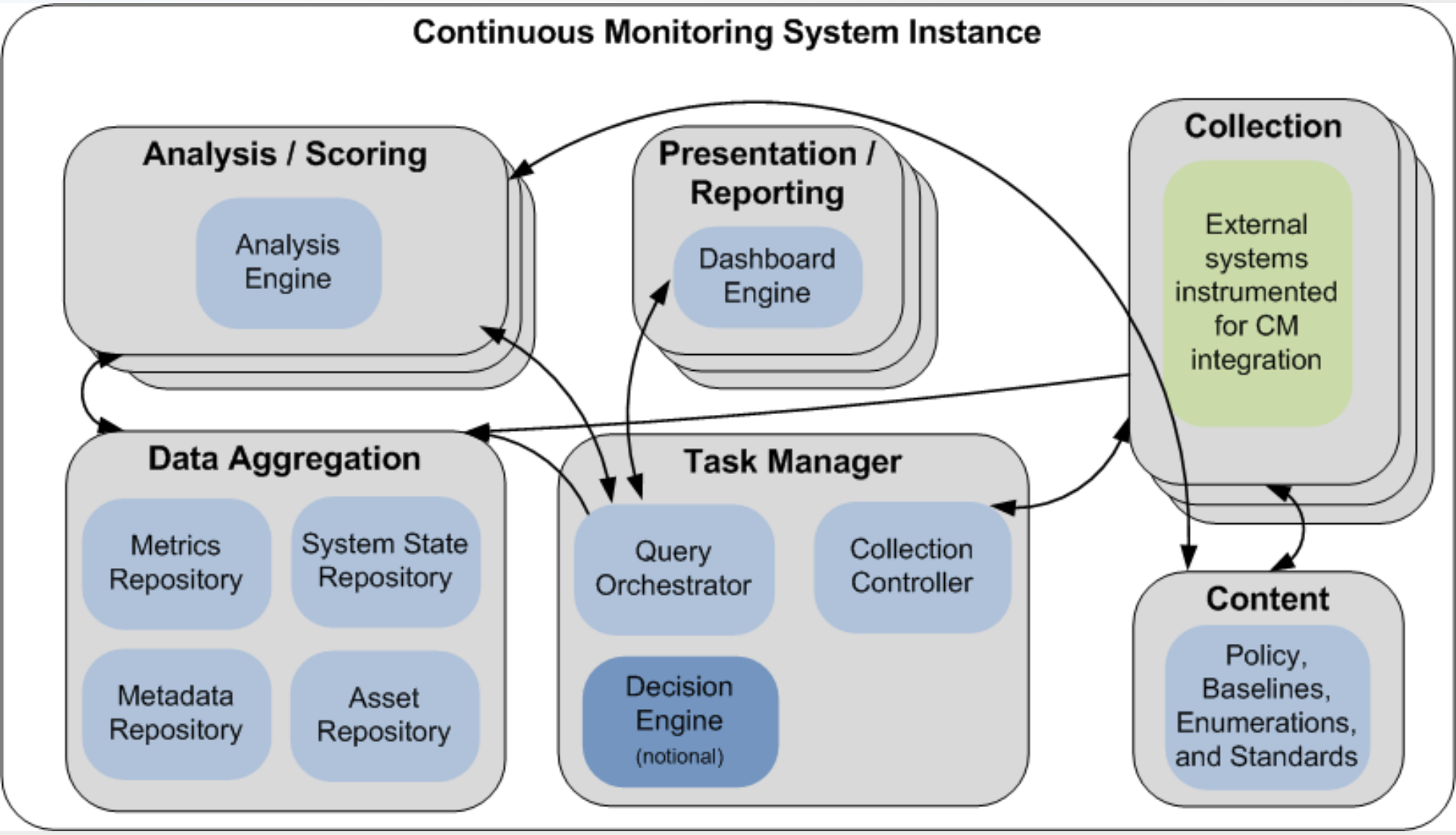
- Define specifications for modular, functional components
- Define interfaces for inter-component communications

Derived Architectures

- Continuous monitoring domains chosen
- Specific systems and software are leveraged
- Number of instances determined

CM Instance Model

(Organizations may have multiple CM instances)

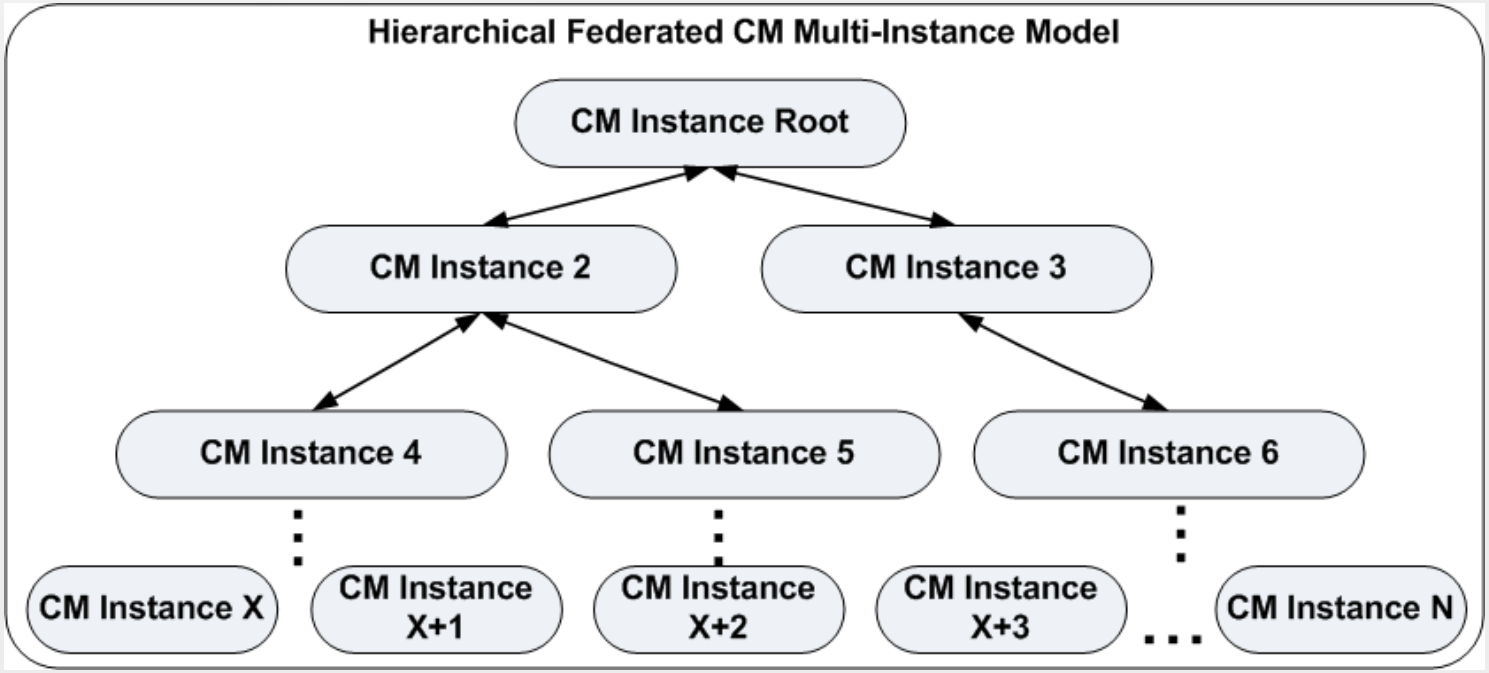


Revised CM Reference Model

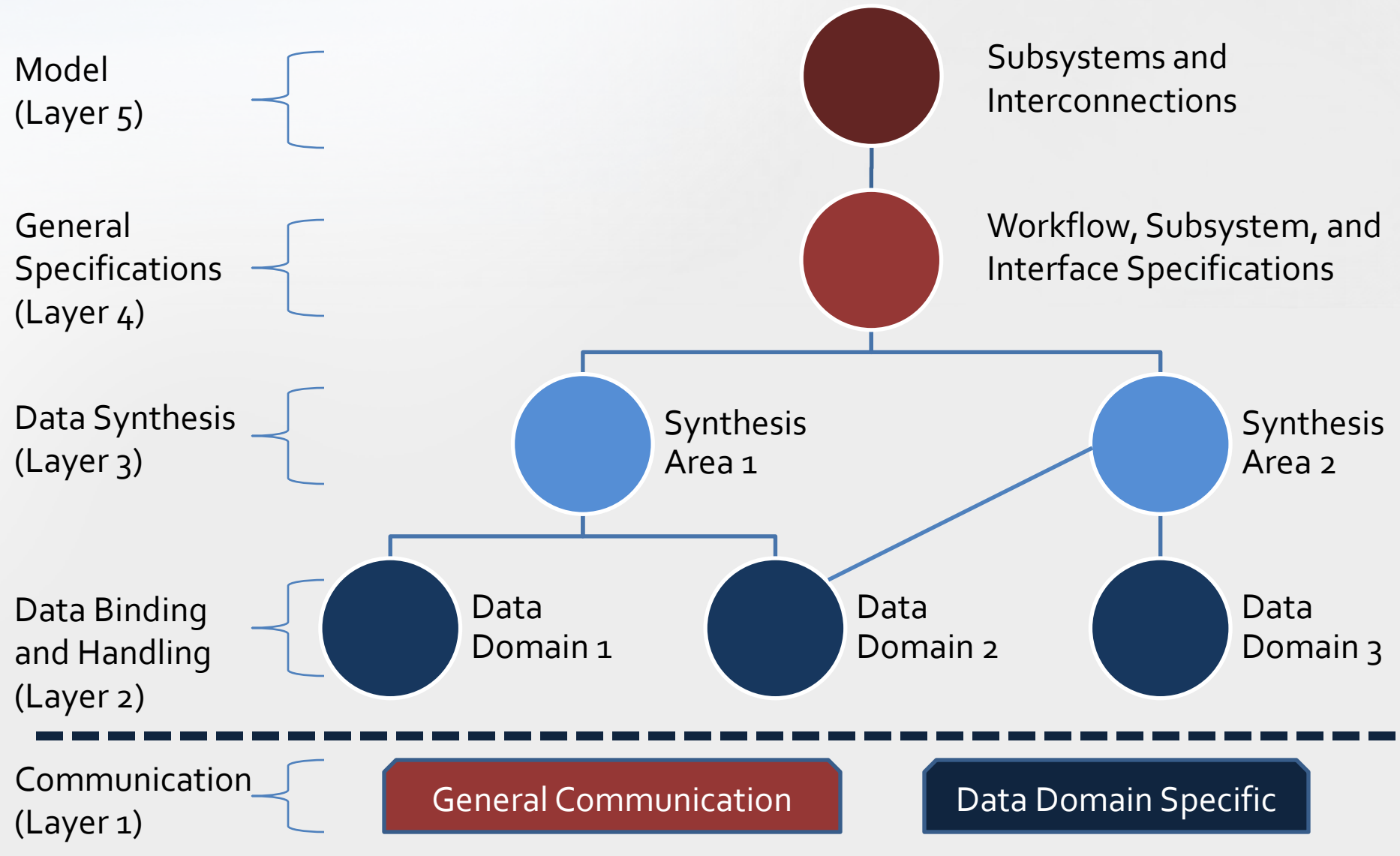
- Six subsystem types
  - **Presentation / Reporting Subsystem (1 or more)**
    - **Dashboards, reports, user queries**
  - **Analysis / Scoring Subsystem (1 or more)**
    - **Data deconfliction, analysis, and scoring**
  - **Data Aggregation Subsystem (1)**
    - **Central repository**
  - **Content Subsystem (0 or 1)**
    - **Holds digital policy and supporting content**
  - **Task Manager Subsystem (1)**
    - **Orchestrates and tasks subsystems to support query resolution**
  - **Collection Subsystem (0 or more)**
    - **Provide feeds of raw data**

Hierarchical Federated Model

- Large organizations may have more than one CM instance
- CM instances are usually arranged in a logical hierarchy
  - Aggregated reports travel up the tree
  - Data calls and configuration requirements travel down the tree
- Often CM instances have a degree of autonomy resulting in a federated style of communication
  - Each instance may have approval authority on directives from higher levels
- Lateral communication in the tree is also possible



CM Specification Model



Layer 5: The Model

- Subsystems
  - Presentation/Reporting
  - Analysis/Scoring
  - Data Aggregation
  - Collection
  - Content
  - Task Management
- Subsystem Components
- Subsystem Interconnections
  - Describes needed communication pathways

Layer 4: General Specifications

- Workflows
  - Data Acquisition and Analysis
  - Query Fulfillment
  - Digital Policy and Content Propagation
- Subsystem Specifications
- Interface Specifications
  - Result Reporting Language
  - Content Acquisition Language
  - Query and Tasking Language
  - Data Retrieval Language

Layer 3: Data Synthesis

- Goal: Extract knowledge from the combination of multiple data domains

- Area 1: Performing multi-data domain analysis and scoring
- Area 2: Creating needed reporting views

Layer 2: Data Binding and Handling

- Specifications describing special handling within the model for data of a specific data domain (e.g., license management)
- Specifications for binding the high level model to data domain specific communication specifications

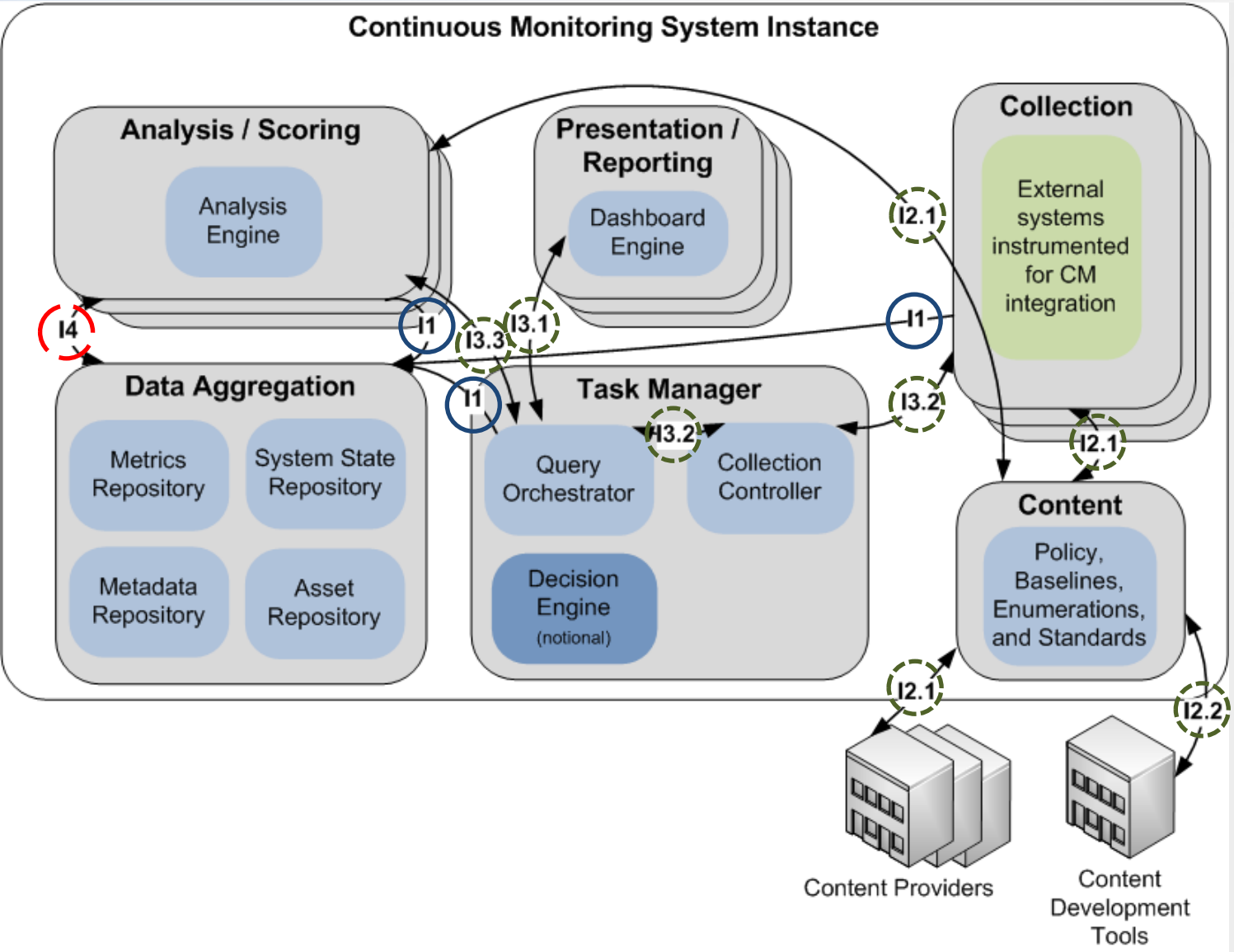
- Initial layer 2 specifications:
  - Asset Management (leveraging the NIST Asset Identification specification)
  - Configuration and Vulnerability Management (leveraging the Security Content Automation Protocol)

Layer 1: Communications

- These are specifications out of scope of the CM modeling work that supply a necessary foundation

- Example Foundation Data Domain Specific Specifications:
  - Security Content Automation Protocol
  - Asset Identification
- Example Foundation Data Domain Agnostic Specifications:
  - Asset Reporting Format

CM Instance Model w/Interfaces



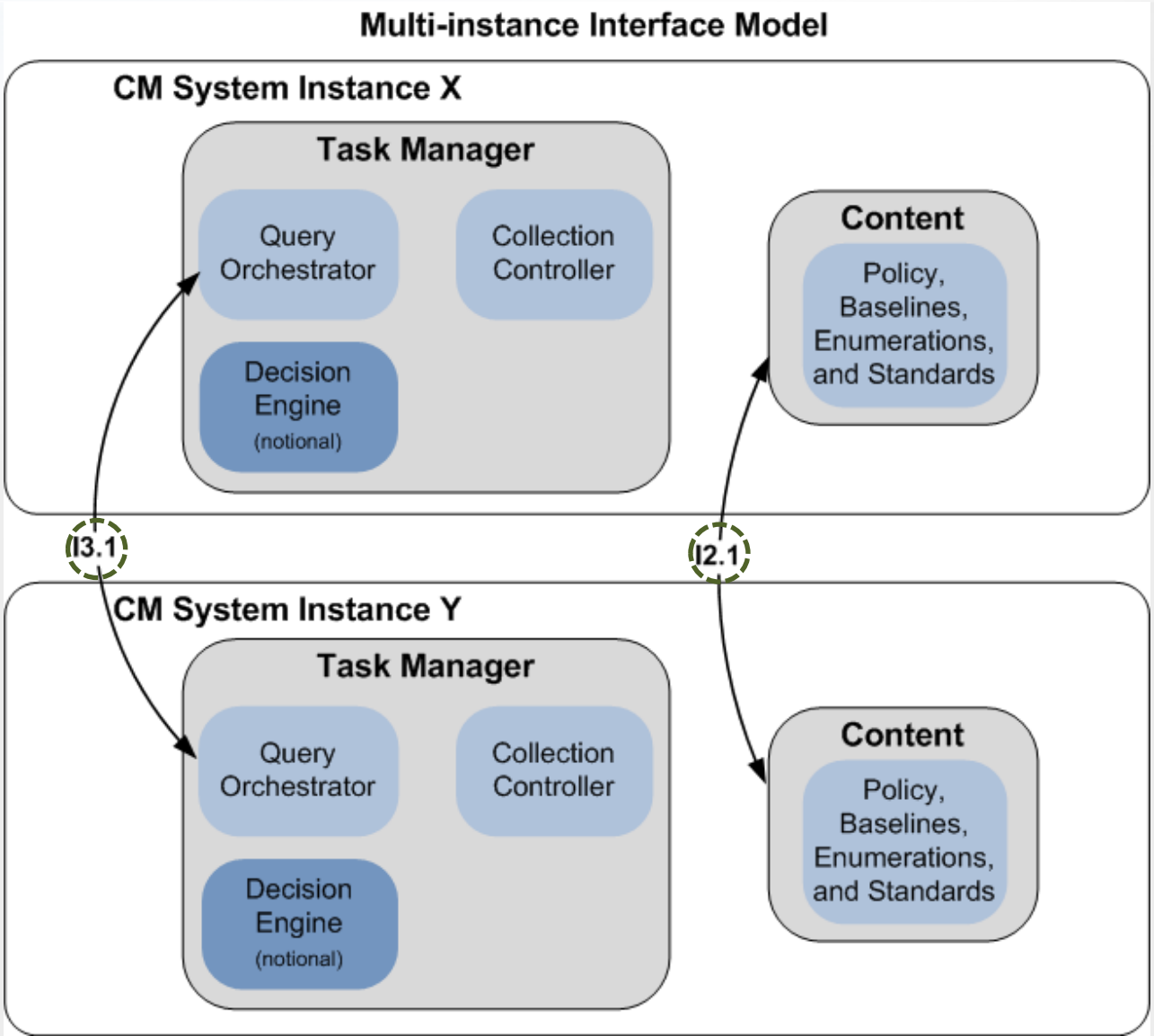
Interface Specifications:

Existing/ Standardized

Current focus/ Parameterized

Future Focus/ Proprietary

CM Multi-instance Model w/Interfaces



Interface Specifications:

Existing/ Standardized

Current focus/ Parameterized

Future Focus/ Proprietary

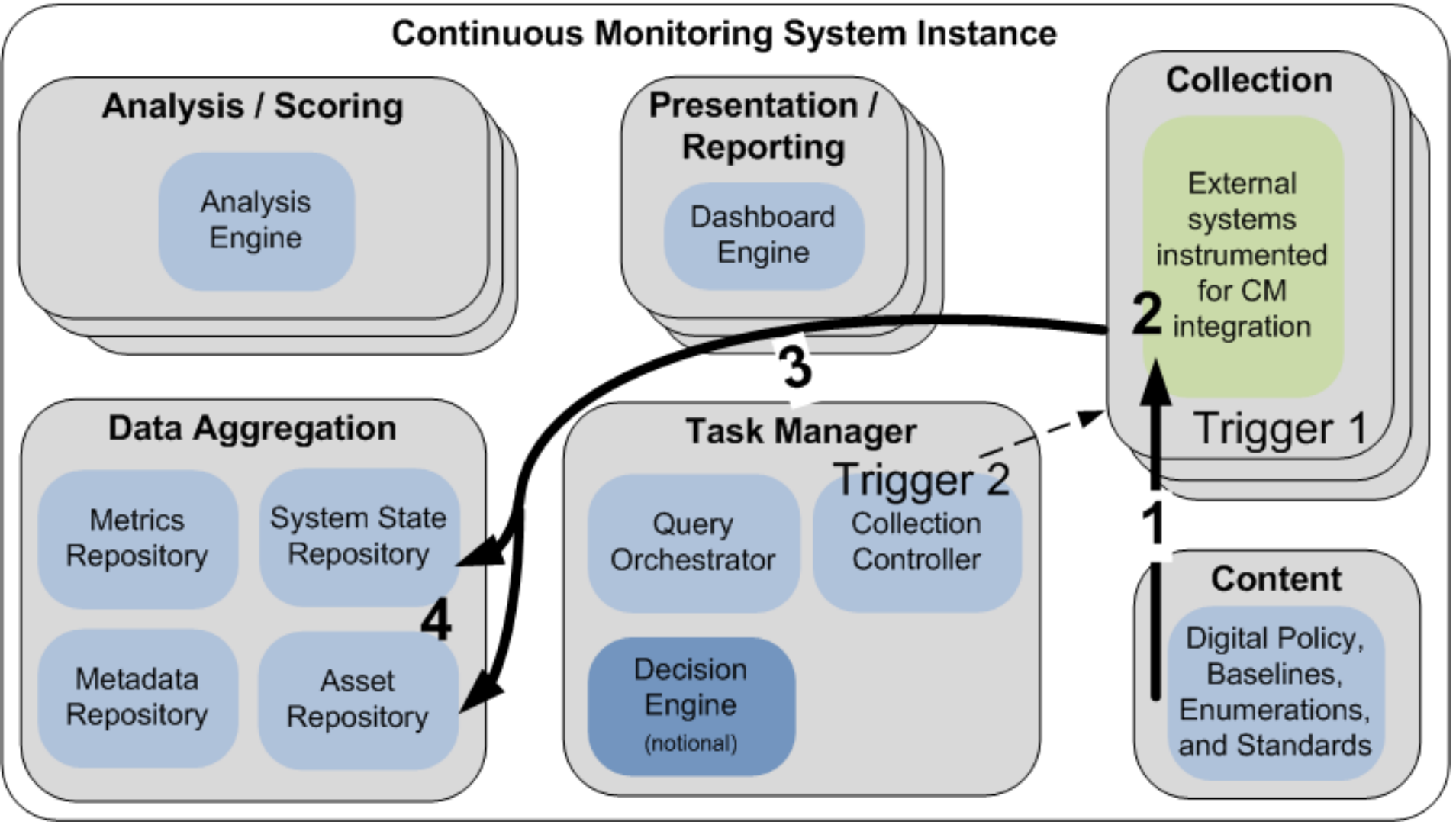
Current Domain Focus

- Configuration and Vulnerability Management
  - Leverage SCAP assessment capabilities providing a standardized enterprise approach
  - Support change management processes
- Asset Management
  - Provide a consolidated asset view across multiple asset repositories
  - Integrate with existing asset management capabilities to:
    - Identify what assets are managed
    - Provide organizational asset metadata
      - Identify responsible parties
      - Provide data in support of analysis and scoring

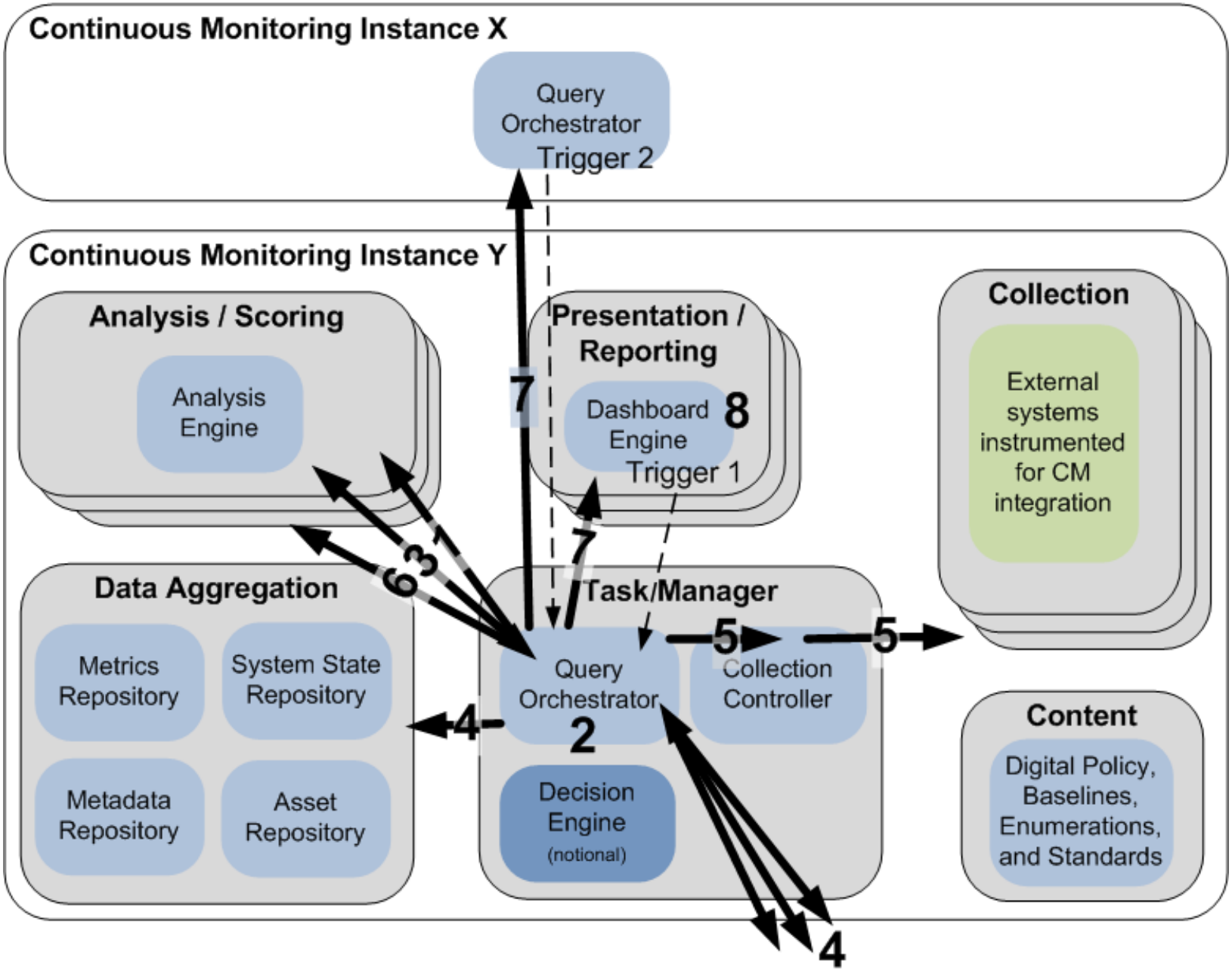
CM Workflows

- **WF1 Data Acquisition**: This workflow describes how raw data is collected and reported to a central repository within a single CM instance.
- **WF2 Query Fulfillment**: This workflow describes how query requests are fulfilled in both single and multi-instance CM architectures. Query fulfillment may include propagation of the query to lower level CM instances, data collection activities, and analysis of collected data.

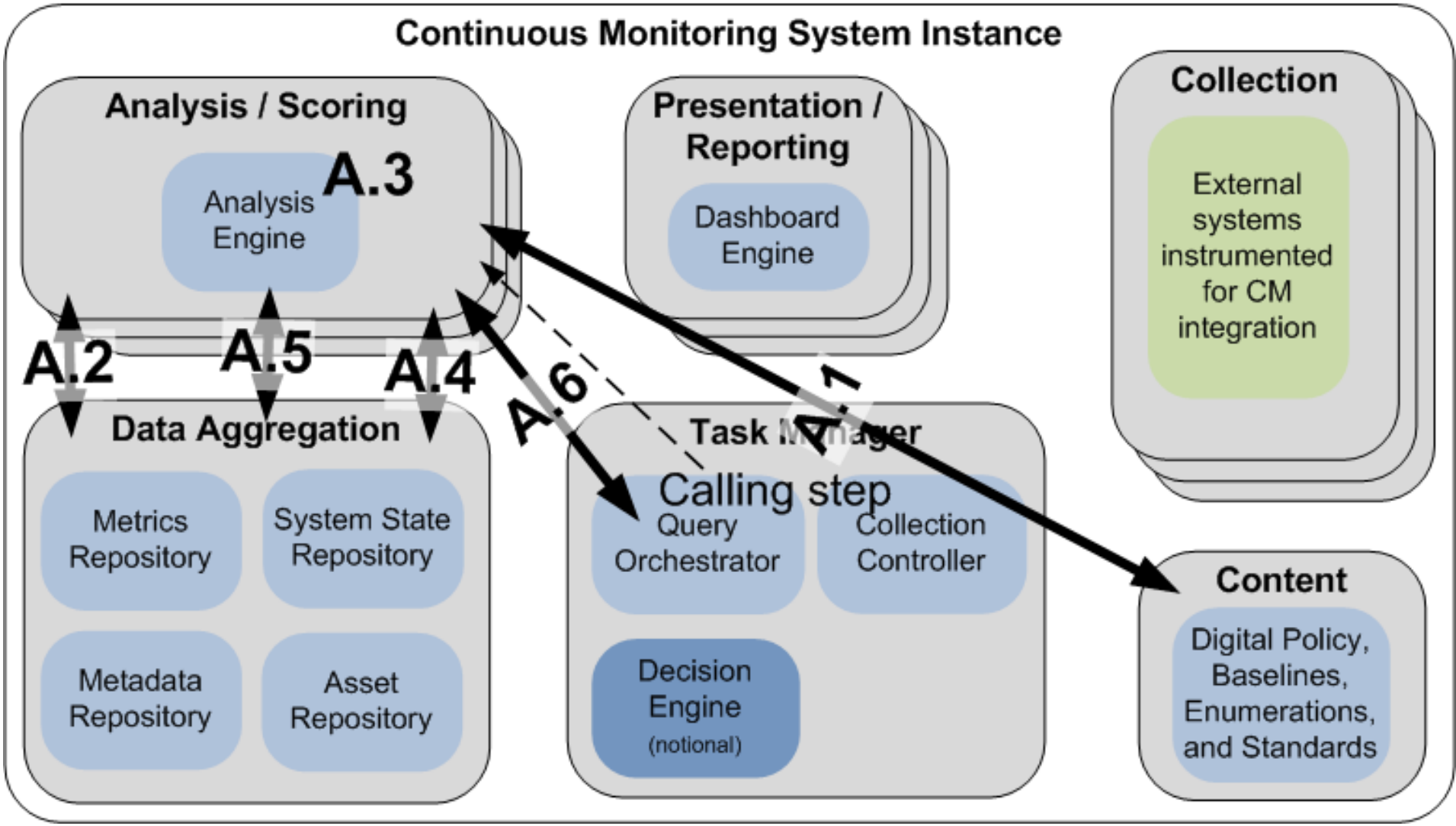
WF1


Continuous Monitoring System Instance
Analysis / Scoring
Analysis Engine
Presentation / Reporting
Dashboard Engine
Collection
External systems instrumented for CM integration
Trigger 1
2
3
1
Data Aggregation
Metrics Repository
System State Repository
4
Metadata Repository
Asset Repository
Task Manager
Trigger 2
Query Orchestrator
Collection Controller
Decision Engine (notional)
Content
Digital Policy, Baselines, Enumerations, and Standards

WF2


Continuous Monitoring Instance X
Query Orchestrator
Trigger 2
Continuous Monitoring Instance Y
Analysis / Scoring
Analysis Engine
Presentation / Reporting
Dashboard Engine
Trigger 1
8
Collection
External systems instrumented for CM integration
7
7
3
6
1
Data Aggregation
Metrics Repository
System State Repository
Metadata Repository
Asset Repository
Task/Manager
Query Orchestrator
2
Collection Controller
Decision Engine
(notional)
5
5
4
4
Content
Digital Policy, Baselines, Enumerations, and Standards

WF2. Analysis Procedure



Integrating Event Management

Discussion Points:

- Where do existing tools and capabilities overlay with the CM subsystem model?
- Where do current approaches differ from this reference model?
- What workflows need to be created or modified to support event management?

Community Teleconference Info

Purpose:

- To share and discuss our thoughts on the creation of a technical reference model for continuous monitoring.
- To generate ideas and feedback from the community to mature the reference model, enabling commercial implementations to be created

Time:

- Thursdays, 1-3pm EDT

Details:

- Weekly read-ahead materials distributed before each call
- Open to any participants

To participate subscribe to emerging-specs@nist.gov at http://scap.nist.gov/community.html.

Closing Thoughts

- There exists great momentum surrounding continuous monitoring (both executive level and grass roots)
  - Dashboards, "big easy" buttons, aggregated reporting of technical metrics
- We desperately need to solve the CM challenge given the vulnerable state of our networks
- The reference model approach provides great benefits:
  - Aids in efficiently addressing known issues
  - Provides situational awareness to differing levels of the organization
  - Reduces integration efforts
  - Implements distributed digital policy and monitoring of that policy
  - Enables orchestration and cooperation of tools (IT TEAMWORK!!)
- The long term vision will take time and effort, but significant gains are achievable today.

Acknowledgements and Credit

- Much of this was inspired and encouraged by others
  - Information Security and Identity Management Committee (ISIMC) Continuous Monitoring working group
  - DHS Federal Network Security (Cyberscope and CAESARS)
  - NSA Information Assurance Directorate (IAD)
  - NIST Security Content Automation Protocol (SCAP) team
  - NIST Risk Management Framework (RMF) team
  - MITRE McLean CAESARS team
  - MITRE Bedford "Making Security Measurable" team

Summary and Questions

Presenter:

David Waltermire
National Institute of Standards and Technology
david.waltermire@nist.gov